DAYBLINK

Navigating the California Consumer Privacy Act

January 2020

INTRODUCTION

What is the California Consumer Privacy Act (CCPA)?

Passed into California law on June 28th, 2018, the CCPA is the strongest privacy legislation enacted in any state at the moment, giving more power to consumers in regards to their personal data. At its core, it aims to provide consumers with the right to know what information businesses collect about them, to tell a business not to share or sell their personal information, and to protections against businesses which do not uphold the value of their privacy.[1]

The compliance deadline for the CCPA went into effect on January 1st, 2020. Organizations affected by its regulations must now undertake efforts to better identify their current data processing activities, and how these may need to be altered to ensure compliance and minimize liability. American companies that managed to skirt the sweeping regulatory demands of GDPR due to a lack of contact with European Union citizen data are much less likely to dodge responsibility stemming from the CCPA, as all data from California residents will fall under the law.

What major similarities exist between the CCPA & the Global Data Protection Regulation (GDPR)?

For organizations who are already subject to GDPR, the degree to which CCPA incorporates elements of GDPR is critical in determining how much further action is required to achieve compliance. Overlaps between the two laws will prove a relief for GDPR subject companies, as it ensures the journey to compliance with CCPA will not start at square one. Importantly, there is significant convergence between the two laws, including the demands for organizations to:

- *Give individuals rights to access and delete their personal information*
- *Require transparency about information use*
- *Necessitate contracts between businesses and their service providers* [2]
- *Require technical controls to prevent re-identification in order to consider data pseudonymized*
- *Take reasonable security measures as protection from data breaches* [3]
- *Provide personal information in a readily usable and transportable format in response to a request for disclosure*

[1]"About the Initiative: California Consumer Privacy Act." *About the Initiative | California Consumer Privacy Act*, www.caprivacy.org/about.
[2]"CCPA vs. GDPR: the Same, Only Different: | Insights: DLA Piper Global Law Firm." *DLA Piper*, 2019, www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/.
[3]Jehl, Laura, and Alan Friel. *CCPA and GDPR Comparison Chart*. www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

GDPR & CCPA: *DISTINCTIONS*

Who is Protected?

GDPR	Data subjects, defined as identified or identifiable persons to which personal data relates.
CCPA	Consumers, defined as California residents that are either in California for other than a temporary or transitory purpose, domiciled in California but are currently outside the state for a temporary or transitory purpose. Consumers include customers of household goods and services, employees, and Business-to-Business transactions.

Key Differences

The laws approach the issue of who falls under protection very differently, but the protections are similarly broad in effect. They both focus on information relating to an identifiable person, but definitions differ slightly. Both laws, however, carry implications for organizations operating outside of the jurisdiction in which the law was passed.

o o o

How is Personal Information Defined?

GDPR	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
CCPA	Any information that identifies, relates to, describes, is capable of being associated with, or could be reasonably linked directly or indirectly, with a particular consumer or household. This covers not only identifiers like name or address, but extends to browsing history, behavioral data, or more.[4]

Key Differences

The GDPR definition covers publicly available data, while the CCPA does not. The GDPR prohibits processing of special categories of personal data, while the CCPA does not make any such distinctions. The GDPR protects personal data related to health at a higher standard, while the CCPA excludes medical data from its protection to the extent that it is governed by the Confidentiality of Medical Information Act.

[4]Hospelhorn, Sarah. "California Consumer Privacy Act (CCPA) vs. GDPR." *Inside Out Security*, 5 Nov. 2018, www.varonis.com/blog/ccpa-vs-gdpr/.

What Rights are Granted to Consumers?

GDPR	• Right to
	  ○ Be informed
	  ○ Deletion
	  ○ Access
	  ○ Object
	  ○ Rectification
	  ○ Restrict processing
	  ○ Data portability
	  ○ Restrict automated individual decision making, including profiling

CCPA	• Right to
	  ○ Be informed
	  ○ Deletion
	  ○ Access
	  ○ Object
	  ○ Non-discrimination for exercise of rights
	  ○ Data portability [5]

Key Differences

Regarding the right to be informed, the CCPA doesn't distinguish between the notice for collecting information directly from individuals and that from obtaining the information from other sources. The CCPA only allows the right to deletion for data that has been collected directly from a consumer. Also, the CCPA only extends the right to object to the *sale* of personal data, where under the GDPR, consumers can object to processing of any type. Also of note is the fact that the GDPR doesn't explicitly outline the right to non-discrimination for the exercise of rights.

o o o

Who Must Comply?

GDPR	Any "data controllers" (who determine the purpose and means of processing the data) and "data processors" (who process the data) that holds personal data of EU citizens.
CCPA	All companies that serve California residents and have at least $25MM in annual revenue ***or*** companies of any size that have personal data on at least 50,000 residents ***or*** collect at least half of their revenue from the sale of personal data [6]

Key Differences

Businesses, public bodies, and institutions, as well as not-for-profit organizations are subject to the GDPR. Only for-profit entities are covered under the CCPA. Also, the CCPA sets thresholds that determine businesses covered by the law, while the GDPR doesn't.

[5]Marini, Alice, et al. *Comparing Privacy Laws: GDPR v. CCPA.*
[6]*California Consumer Privacy Act (CCPA): What you need to know to be compliant, CSO*

What is the Basis for Consent?

GDPR	Requires consumers to opt-in to data collection by instructing sites to get consent before collecting data.
CCPA	Allows sites to collect and sell data if the consumer signs up or makes an online purchase, and only offers consumers the right to opt-out.

Key Differences

Though both laws afford consumers similar rights to opt-out in instances where processors are using their data for sale, the default settings are more structurally protective of consumers in the GDPR.

o o o

What is the Acceptable Response Time to a Consumer Request for Data?

GDPR	Responsible parties have 40 days to respond to a request for data.
CCPA	Responsible parties have 45 days to respond to a request for data. Consumers have the right to request all the data a company has collected on them over the previous 12 months.

Key Differences

Although time frames are similar (5 more days under CCPA), the CCPA's request guidelines are broader in scope than GDPR and can include contact info for all 3rd parties to which data is sold

o o o

What Financial Penalties Exist?

GDPR	Organizations found to be in violation can be fined up to 4% of annual global turnover, or €20 Million.
CCPA	Organizations found to be in violation can be fined up to $2,500 per violation for negligent violations and up to $7,500 per violation for intentional violations.

Key Differences

CCPA fines are likely to be much smaller than GDPR fines.That being said, CCPA does not provide explicit total maximum fines that can be incurred.

ROADMAP TO COMPLIANCE

10 Things Organizations Should Do Now

1. Know One's Obligation to CCPA

Before organizations do anything else, they should ensure a fundamental understanding of the ways in which they are impacted by the CCPA. The law provides the following conditions to clarify which types of organizations are obligated to comply.

The organization:

- Collects consumers' personal information
- Determines how and why that information is processed
- Conducts business in California, even if only online
- Meets one of the following annual criteria:
    - Gross revenue of at least $25 million
    - Collects personal information for at least 50,000 consumers, households, or devices
    - Derives half of its annual revenue from the sale of personal information

Those that do not meet these conditions fall outside of the legislation's reach.

2. Understand Gaps Between CCPA and GDPR

The notion that if an organization has achieved GDPR compliance, it is automatically CCPA compliant, though tempting, is false. As discussed, just because the GDPR is broadly perceived to be more extensive in a regulatory sense does not mean that the CCPA does not require different or further action in several key areas of interest. Therefore, it is in the best interest of organizations with a duty to comply with both laws to coordinate their GDPR and CCPA compliance efforts, while remaining acutely aware of the distinctions.

Both laws require a thorough assessment of data inventories and processing workflows, which provides an opportunity to save time by completing and utilizing such due diligence in a way that adds value to the compliance efforts towards both the GDPR and the CCPA. In several cases, however, there is language within the CCPA that simply does not exist in the GDPR, and thus demands not only additional attention, but additional execution beyond the compliance efforts made for GDPR.

3. Take Inventory of Personal Data

In order to comply with CCPA, businesses must first understand their data collection streams and storage processes, and identify which types of that data qualify as "personal information".

The Chronicle of Data Protection recommends the following questions be asked to carry out a rigorous assessment of current data practices:[6]

- What personal information do you collect or possess?
- How do you collect it?
- Where and how do you store it?
- Do you share it with other entities?
- Is such shared data part of a sale, a provision of service, or used for some other purpose?

Additionally, all categories of personal information being received should be identified. For each category identified:

- Pinpoint the source of the information (third party, your own observations, directly from the individual)
- Identify the purpose and use for the collection of the data
- Identify the length of time each category is legally required to be retained in order to honor deletion requests of customers
- Locate where the information is being stored
- Identify in which format the information is being stored
- Identify the person responsible for maintaining the information

4. Prepare Privacy Disclosures

A central pillar of the CCPA is the notion that consumers have the right to know the data that is being collected from them. This right manifests itself through the requirement that businesses must disclose which data they are collecting at or before the point of collection. This disclosure notice must "inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used."[7]

Businesses must additionally disclose where that personal information is gathered from, the categories of third parties with whom it is shared, and any specific pieces of personal information collected. These disclosures need to be ready for deployment by January 1st, 2020, and should be available through a publicly posted privacy notice, and specifically upon request by a consumer.

[6]Meyer, Catherine D., and Fusae Nara. "Countdown to CCPA: Do You Know Where Your Data Is?" *Pillsbury Law*, 1 May 2019, www.pillsburylaw.com/en/news-and-insights/ccpa-data-inventory.html.
[7]Cwalina, Chris, et al. "California Consumer Privacy Act: Disclosure Requirements." *Data Protection Report*, 18 June 2019, www.dataprotectionreport.com/2018/09/california-consumer-privacy-act-disclosure-requirements/.

5. Create a Home Page Privacy Link

In the CCPA's efforts to protect consumer data privacy, the legislation includes a requirement for all covered businesses to install a privacy link on the homepage of its website. The link must be "clear and conspicuous", titled "Do Not Sell My Information" and linked to a page that allows consumers to opt out of having their personal information sold. Importantly, this requirement only applies to businesses that "sell" personal information about California consumers to third parties. However, "sell" as CCPA defines it does not mean "sell" as many understand. Rather, it means share for any benefit at all.[8]

Covered entities should begin the IT change management process for installing this link on their homepage as soon as possible, because it should have been visible as of January 1st, 2020. Furthermore, the website's landing page is not the only place where this link must appear. Businesses are also required to install it in their online privacy policies if applicable, and any California-specific description of consumers' privacy rights.

6. Create a Process for Consumer Requests

Beginning January 1st, 2020, covered businesses must be prepared to respond to consumer requests about their personal information that are facilitated by the CCPA. The requests must be processed free of charge, and within 45 days. This creates the need for covered entities to develop appropriate procedures for processing the following types of consumer inquiries:

- Request a copy of their personal information
- Request that their personal information be deleted
- Find out what categories of their personal information are being sold
- Request to opt out of the sale of personal information for those over 16 years old
- Request to opt in for the sale of personal information for those between the age of 13 and 16
- Obtain consent from a guardian to sell personal information from a consumer under 13 years old

It is critical that businesses take heed of the listed age requirements, because the law states that "a business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age".

[8]"The CCPA Has Placed a Mandatory Link on Your Company's Homepage." *JD Supra*, www.jdsupra.com/legalnews/the-ccpa-has-placed-a-mandatory-link-on-61019/.

7. Strengthen Data Security

Because the CCPA allows consumers to seek damages for compromised personal information if it is the result of the business' violation of the duty to implement and maintain reasonable security procedures and practices", the consequences of a privacy breach become far more threatening. To protect themselves against such a breach, businesses should review and update their information security and privacy policies and actively monitor their data security defenses to ensure this risk is mitigated to the greatest extent possible.

Though it is not explicitly clear what levels of data security are required to relieve an organization of blame come a cyber attack, the #1 recommendation from California's Attorney General in the 2016 "California Data Breach Report" is to implement a cybersecurity framework.[9] The report recommends that "organizations implement the 20 controls in the Center for Internet Security's Critical Security Controls", affirmatively stating that "the failure to implement such controls would constitute a lack of reasonable security". Organizations should, therefore, begin by assessing and implementing these 20 controls.

8. Assess Third Parties

Crucially, a business is provided with a safe harbor for non-compliance by their service providers if certain controls with the service provider have been put in place. Therefore, it is appropriate to address all third parties with whom the business is working and the contracts with such third parties, both in terms of parties to whom data is transferred and counter-parties when the business is a recipient of data.[10]

It is critical to

- Identify all entities that are given access to personal information
    - Confirm whether a contract is in place with each entity
        - Confirm that the contract language is supportive of CCPA
    - Confirm the purpose of such access
    - Confirm whether the entity may use the information for its own commercial purposes
- Open a dialogue regarding your business's CCPA requirements and how they impact the relationship
- Create a third party CCPA due diligence process for each third party
    - Use a scorecard or assessment tool built to address key risk concerns
    - Plan for ongoing monitoring
- Add CCPA elements to your business continuity plans

[9]Brynn, Sera. *Data Security under the California Consumer Privacy Act: Instructions Not Included: Sera-Brynn*. 7 May 2019, sera-brynn.com/data-security-under-the-california-consumer-privacy-act-instructions-not-included/.
[10]"7 Steps to Success for Ensuring Third-Party CCPA Compliance." *Aravo*, www.aravo.com/blog/7-steps-to-success-for-ensuring-third-party-ccpa-compliance/.

9. Train Employees

Once a business has updated its IT systems and processes, it is imperative that employees are made aware of the key aspects of the CPCA, and corresponding procedural updates. This education should have taken place before January 1st, 2020, and should produce employees that understand the following:

- Their physical location or that of company headquarters does not determine CCPA coverage
- How the way they must handle consumer data is practically changing
- For this law's purposes, a consumer is a resident of California
- Where to direct or how to process consumer requests regarding their personal information
- Whether the organization has decided to apply this law across its entire footprint for consistency sake or only to California consumers

10. Stay Up-to-Date with Federal and State Privacy Developments

Unfortunately for businesses for whom compliance with privacy laws like the CCPA is a major pain point, the CCPA is far from the last of these legislative efforts that will require adaptation. There are a variety of state laws with similar aims to the CCPA which are pending in states such as Washington State and New York.[11] These bills include various versions of opt-out rights, and require new disclosure requirements that are distinct from those of GDPR or CCPA, threatening to greatly complicate compliance efforts for businesses subject to multiple privacy laws.

The federal government has also introduced a multitude of privacy bills into its legislative chambers, such as one that can preempt state laws, including the CCPA. It is of critical importance that businesses stay current on legislative privacy developments, and keep their data processing procedures agile enough to readily adapt to major changes in the legislative landscape. Additionally, it is advised that businesses remain in frequent contact with their privacy counsel, who are more equipped to understand appropriate courses of action prompted by changes in the privacy legislative landscape.

[11] "GDPR, CCPA and beyond: Changes in Data Privacy Laws and Enforcement Risks to Monitor in 2019." *Data Protection Report*, 18 June 2019, www.dataprotectionreport.com/2019/02/gdpr-ccpa-and-beyond-changes-in-data-privacy-laws-and-enforcement-risks-to-monitor-in-2019/.

ABOUT THE AUTHORS

Justin Whitaker is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence and is based in the Vienna, Virginia office.

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence, a former cybersecurity entrepreneur, and is based in the Vienna, Virginia office.

Jacob Armijo, CISM is a Senior Consultant at DayBlink and Chief of Staff of DayBlink's Cybersecurity Center of Excellence. He is based in the Vienna, Virginia office.

Research contributions from: Harry Baker, Chloe Spetalnick, Clare Suter, and DayBlink's Cybersecurity Center of Excellence

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It is outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored and living in the cloud, and constant mobile demand. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security and privacy posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cyber@dayblink.com
Call: 1 (866) 281-4403